

520.43249X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Kiyoto, et al
Serial No.:
Filed: October 30, 2003
Title: PEER-TO-PEER COMMUNICATION APPARATUS AND
COMMUNICATION METHOD
Group:

LETTER CLAIMING RIGHT OF PRIORITY

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

October 30, 2003

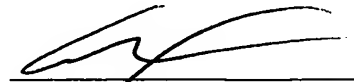
Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 2003-064328 filed March 11, 2003.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Carl I. Brundidge
Registration No. 29,621

CIB/nac
Attachment
(703) 312-6600

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 1 1 日
Date of Application:

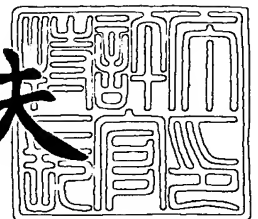
出 願 番 号 特 願 2 0 0 3 - 0 6 4 3 2 8
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 0 6 4 3 2 8]

出 願 人 株式会社日立製作所
Applicant(s):

2 0 0 3 年 9 月 2 9 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 7 9 7 1 4

【書類名】 特許願

【整理番号】 K02016021A

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/28

【発明者】

【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 ネットワークソリューション事業部内

【氏名】 清藤 聡史

【発明者】

【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 ネットワークソリューション事業部内

【氏名】 星野 和義

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所 中央研究所内

【氏名】 湯本 一磨

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所 中央研究所内

【氏名】 日高 稔

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ピアツーピア通信装置および通信方法

【特許請求の範囲】

【請求項 1】

IP ネットワークに接続され、1 対 1 の対等型通信を行うピアツーピア通信装置であって、

前記 IP ネットワークに接続された他の通信装置が属するネットワークに関する情報と、前記他の通信装置の利用者に関する情報とを含む第 1 の制御情報を取得する手段と、

前記 IP ネットワークに接続された他の通信装置の通信パケットの送受信における暗号規則と認証規則とを含む第 2 の制御情報を取得する手段と、
を備え、

前記第 1 の制御情報と前記第 2 の制御情報とから、前記他の通信装置に送信する IP パケットのセキュリティポリシーを決定し、前記決定したセキュリティポリシーを用いて前記他の通信装置に IP パケットを送信することを特徴とするピアツーピア通信装置。

【請求項 2】

請求項 1 に記載のピアツーピア通信装置であって、
前記取得した第 1 の制御情報を記憶する手段と、
前記取得した第 2 の制御情報を記憶する手段と、
をさらに備えたことを特徴とするピアツーピア通信装置。

【請求項 3】

請求項 1 もしくは 2 に記載のピアツーピア通信装置であって、
前記決定した、送信 IP パケットに関する第 2 の制御情報を、前記他の通信装置に通知する手段をさらに備えたことを特徴とするピアツーピア通信装置。

【請求項 4】

請求項 1 乃至 3 に記載のピアツーピア通信装置であって、
前記取得した第 1 の制御情報と前記取得した第 2 の制御情報とを表示し、前記新たに決定したセキュリティポリシーを入力する外部インタフェース手段をさらに

備えたことを特徴とするピアツーピア通信装置。

【請求項 5】

I P ネットワークに接続され、I P パケットを用いて 1 対 1 の対等型通信を行うピアツーピア通信装置であって、

前記 I P パケットの終端および生成を行う I P 機能部と、

前記 I P パケットに対する認証および暗号化を処理する I P s e c 機能部と、

通信装置間におけるピアツーピア通信の確立および切断を処理するピアツーピア通信機能部と、

前記 I P ネットワークに接続された他の通信装置が属するネットワークおよび前記他の通信装置の利用者に関するプレゼンス情報を格納するプレゼンス情報記憶部と、

前記プレゼンス情報記憶部へのアクセスを制御するプレゼンス情報処理部と、

前記 I P ネットワークに接続された他の通信装置の通信パケットの送受信における一連の暗号および認証規則を示すセキュリティポリシー情報を格納するセキュリティポリシー情報記憶部と、

前記セキュリティポリシー情報記憶部へのアクセスを制御するセキュリティポリシー処理部と、

使用者からのセキュリティポリシーおよびプレゼンス情報の取得要求を行う第 1 のインタフェース部と、

使用者の、前記セキュリティポリシー情報記憶部へのアクセスを行う第 2 のインタフェース部と、

使用者の、前記プレゼンス情報記憶部へのアクセスを行う第 3 のインタフェース部と、
を備え、

前記プレゼンス情報と前記セキュリティポリシー情報とから、前記他の通信装置に送信する I P パケットのセキュリティポリシーを決定し、前記決定したセキュリティポリシーを用いて前記他の通信装置に I P パケットを送信することを特徴とするピアツーピア通信装置。

【請求項 6】

I P ネットワークにおける 1 対 1 の対等型通信を行う通信方法であって、
前記 I P ネットワークに接続された他の通信装置が属するネットワークに関する情報と、前記他の通信装置の利用者に関する情報とを含む第 1 の制御情報を取得し、
前記 I P ネットワークに接続された他の通信装置の通信パケットの送受信における暗号規則と認証規則とを含む第 2 の制御情報を取得し、
前記第 1 の制御情報と前記第 2 の制御情報とから、前記他の通信装置に送信する I P パケットのセキュリティポリシーを決定し、
前記決定したセキュリティポリシーを用いて前記他の通信装置に I P パケットを送信する
ことを特徴とする通信方法。

【請求項 7】

請求項 6 に記載の通信方法であって、
前記決定した、送信 I P パケットのセキュリティポリシー情報を、前記他の通信装置に通知する段階をさらに備えたことを特徴とする通信方法。

【発明の詳細な説明】**【0 0 0 1】****【発明の属する技術分野】**

本発明は、1対1の対等型ピアツーピア通信装置に関し、特に、通信相手や通信相手のネットワーク状況に応じた最適な通信セキュリティ規則を適用するピアツーピア通信装置に関する。

【0 0 0 2】**【従来の技術】**

インターネット電話を代表とするピアツーピア通信において、第三者によって通信内容を盗聴または改竄されることを防ぐために、通信パケットの暗号化や認証が行われる。通信パケットの暗号化や認証は、個々の通信パケットに対してどのような暗号化や認証を行うかといった一連の規則であるセキュリティポリシーに従って行われる。なお、このようなセキュリティポリシーを格納するデータベースをセキュリティポリシーデータベースといい、通常、別途設置されたポリシーサー

バと呼ばれる装置に格納されている。

【0003】

インターネット技術の標準化組織である I E T F では、インターネットにおける I P (I n t e r n e t P r o t o c o l) パケットレベルでのセキュリティ (第三者による通信内容の盗聴や改竄等の防止) を確保するプロトコルとして I P s e c (I P s e c u r i t y) を策定している (非特許文献 1 参照)。

【0004】

これによれば、送信元および送信先の I P アドレスとポート番号、T C P (T r a n s m i s s i o n C o n t r o l P r o t o c o l) や U D P (U s e r D a t a g r a m P r o t o c o l) といった上位層プロトコルの種別、受信パケットか送信パケットかを示す通信の方向といった情報を用いて、当該ピアツーピア通信に適用すべきセキュリティポリシーを選択する。

【0005】

そして、選択したセキュリティポリシーに記述されているセキュリティ要件 (パケットを破棄するかしないか、暗号化を行うか認証を行うか、必ず行うか可能な場合のみ行うか等) が適用される。すなわち、送信側の装置は、送信するパケットの送信元アドレスや送信先アドレスから、セキュリティポリシーデータベースを検索し、該当するセキュリティポリシーにて示されるセキュリティ要件を満たす暗号化や認証処理を行った後、通信相手にパケットを送信する。

【0006】

同様に、受信側の装置は、受信したパケットの送信元アドレスや送信先アドレスから、セキュリティポリシーデータベースを検索し、受信パケットが該当するセキュリティポリシーにて示されるセキュリティ要件を満たす暗号化や認証処理が行われているかを検査し、セキュリティ要件を満たしていないパケットは上位層に渡すことなく廃棄する。

【0007】

インターネットを用いて、2つの通信ノード間で仮想的な専用線を確立する V P N (V i r t u a l P r i v a t e N e t w o r k) において、I P s e

c を用いて通信のセキュリティを確保する技術としては、例えば、非特許文献 2 に開示されているものがある。

【0 0 0 8】

【非特許文献 1】

I E T F R F C 2 4 0 1、1 9 9 8 年 1 1 月 2 5 日、p. 1 4 - 1 7

【非特許文献 2】

石井貴之、他 1 名、「透過的で動的な V P N メカニズムを実現」、季刊 I P v 6 マガジン、株式会社インプレス、平成 1 4 年 8 月 1 8 日、S u m m e r 2 0 0 2 N O . 2、p. 7 4 - 7 5

【0 0 0 9】

【発明が解決しようとする課題】

上記非特許文献 1 に記載の I P s e c を適用したピアツーピア通信では、送信側装置に登録されているセキュリティポリシーのセキュリティ要件が、受信側装置に登録されている要件を満たさない場合、送信側装置が送信したパケットは受信側装置にて受信後廃棄される。従って、相手装置と適切に通信を行うためには、予め通信装置間において互いのセキュリティポリシーを交渉または交換し、通信相手装置のセキュリティ要件を満たすセキュリティポリシーに基づいて通信を行う必要がある。

【0 0 1 0】

また、モバイル端末装置によるピアツーピア通信のように、通信相手装置が同一の場合であったとしても、それが社内ネットワークに接続されている場合には相応のセキュリティが確保済みと考えられるため、セキュリティレベルを落としたセキュリティポリシーを用いて暗号処理等を必要としないより軽快な通信を行い、通信相手端末が社外ネットワークに接続されている場合には、よりセキュリティレベルの高いセキュリティポリシーを用いた通信が望まれる。

【0 0 1 1】

さらに、通信相手が家族や友人・知人かそうでないか、通信内容がビジネスかプライベートか、また単なる宣伝・広告か等により、適切なセキュリティレベルによる通信が期待できる。

【 0 0 1 2 】

しかしながら、通信相手が上述のような各種状況に応じて適切なセキュリティポリシーを作成し設定しているとは限らない。例えば、社内ネットワークに接続されたモバイル端末装置が移動し、接続先が社外ネットワークに切り替えられた際、セキュリティポリシーが従前の社内ネットワークに適した比較的緩いセキュリティ要件のままであった場合、第 3 者等によって通信パケットを盗聴や改竄される危険性が高くなる。

【 0 0 1 3 】

一方、非特許文献 2 に記載の技術では、ネットワーク上に設けた外部の I P s e c 通信管理サーバを介して、通信装置相互間でセキュリティポリシー情報の送受信、およびネゴシエーションを行っている。

【 0 0 1 4 】

しかしながら、外部に設置したサーバを用いているため、サーバにてネットワーク上の通信セキュリティポリシーを集中的に管理し、通信装置がセキュリティポリシーの変更を行えないという問題があり、利用者が通信状況に応じてセキュリティポリシーを自由に設定するといった柔軟的な機能を提供することは不可能であった。

【 0 0 1 5 】

本発明では、通信パケットに対する暗号および認証規則を示す情報であるセキュリティポリシーと、通信端末の接続ネットワークの情報や通信相手の情報および通信内容の情報といった通信端末の状態を示す情報であるプレゼンス情報とを、通信装置間で互いに交換し、通信状況に応じた適切なセキュリティポリシーによって、通信の安全性が確保されたピアツーピア通信を可能とする通信装置を提供することを課題とする。

【 0 0 1 6 】

さらに、利用者が通信状況に応じてセキュリティポリシーを自由に設定することを可能とする通信装置を提供することを課題とする。

【 0 0 1 7 】

【課題を解決するための手段】

上記課題を解決するために本発明では、IPネットワークに接続された他の通信装置が属するネットワークおよび前記他の通信装置の利用者に関するプレゼンス情報を取得する手段と、前記他の通信装置の通信パケットの送受信における一連の暗号および認証規則を示すセキュリティポリシー情報を取得する手段とを備え、前記プレゼンス情報と前記セキュリティポリシー情報とから、前記他の通信装置に送信するIPパケットのセキュリティポリシーを決定し、前記決定したセキュリティポリシーを用いて前記他の通信装置にIPパケットを送信するようにした。

【0018】

また、前記取得したプレゼンス情報と前記取得したセキュリティポリシー情報とから新たに決定した送信IPパケットのセキュリティポリシー情報を、前記他の通信装置に通知する構成とした。

【0019】

さらに、前記取得したプレゼンス情報と前記取得したセキュリティポリシー情報とを表示し、前記新たに決定したセキュリティポリシー情報を入力するために周辺機器との外部インタフェースをさらに設けた。

【0020】

【発明の実施の形態】

以下、本発明の実施形態について説明する。ここでは、通信網としてIPネットワークを用い、通信の安全性を確保するプロトコルとしてIPsecを用いた場合を例として説明する。

【0021】

図1は本発明の通信装置10の内部構成を説明する図である。本通信装置10はIPネットワーク1を介して通信相手装置11と通信を行う。なお、図1の通信装置10は、以下に説明するセキュリティポリシーの設定等に係る機能ブロックを中心に示したものであり、実際には、モバイル用PCやIP電話といった通信装置の種別によって異なる、他の図示しない機能ブロックを有している。また、通信相手装置11も本通信装置10と同一の機能構成を有するものとする。

【0022】

本発明の通信装置10は、IP機能ブロック100、IPsec機能ブロック

110、ピアツーピア通信機能ブロック200、セキュリティポリシデータベース300、セキュリティポリシ処理部301、セキュリティポリシ入出力I/F302、プレゼンス情報データベース400、プレゼンス情報処理部401、プレゼンス情報入出力I/F402、セキュリティポリシプレゼンス情報要求指示I/F403から構成される。

【0023】

IP機能ブロック100はデータパケットの送受信インタフェースであり、IPパケットの終端および生成を行う。IPsec機能ブロック110はIPレイヤでのセキュリティを確保する機能ブロックであり、IPパケットに対する認証および暗号化を行う。ピアツーピア通信機能ブロック200はピアツーピア通信を実現する機能ブロックであり、通信装置間でのピアツーピア通信セッションの確立、確立したセッション上でのピアツーピア通信、および確立セッションの切断を行う。

【0024】

セキュリティポリシデータベース300は通信端末のセキュリティポリシを格納したデータベースであり、IPsec機能ブロックにて適用するセキュリティポリシの管理を行う。セキュリティポリシ処理部301はセキュリティポリシデータベースへのアクセスを行う機能ブロックであり、セキュリティポリシデータベースへのセキュリティポリシの登録や削除、ならびに参照を行う。セキュリティポリシ入出力インタフェース302はセキュリティポリシデータベースへのアクセスのためのユーザインタフェースであり、利用者に対し通信装置のセキュリティポリシデータベースへのアクセスを提供する。

【0025】

セキュリティポリシプレゼンス情報要求指示インタフェース403はセキュリティポリシおよびプレゼンス情報の取得要求を行うためのユーザインタフェースであり、周辺機器20等を介して、利用者に対し通信相手装置のセキュリティポリシやプレゼンス情報の取得要求を可能とする。プレゼンス情報データベース400は通信端末のプレゼンス情報を格納したデータベースであり、通信装置のプレゼンス情報の管理を行う。

【0026】

プレゼンス情報処理部 401 はプレゼンス情報データベースへのアクセスを行う機能ブロックであり、プレゼンス情報データベースへのプレゼンス情報の登録削除や参照を行う。プレゼンス情報入出力インタフェース 402 はプレゼンス情報データベースへのアクセスのためのユーザインタフェースであり、利用者に対し通信装置のプレゼンス情報データベースへのアクセス機能の提供を行う。

【0027】

なお、上記のセキュリティポリシ入出力インタフェース 302、セキュリティポリシプレゼンス情報要求指示インタフェース 403 およびプレゼンス情報入出力インタフェース 402 は、外部に別途用意されたディスプレイ装置、キーボード、マウス等の周辺機器 20 に接続され、例えば、キーボードやマウス等を用いて各種情報の入力を行ったり、ディスプレイ装置を用いて出力情報の表示を行うことができる。

【0028】

図 2 は通信装置 10 が適用されるネットワーク構成を示す図である。ここでは、利用者 9 が通信装置 10 を用い、社内ネットワーク 2 を介して通信相手装置 A 11-1 とピアツーピア通信を行う場合と、社内ネットワーク 2 およびインターネット 3 を介して通信相手装置 B 11-2 とピアツーピア通信を行う場合とを示している。

【0029】

なお、通信装置 10 および通信相手装置 A 11-1 の IP アドレスとしては、インターネットの標準化組織である IETF にて制定された RFC 1597 に規定されたクラス C のプライベートアドレスを想定し、それぞれ 192. 168. 1. 1 および 192. 168. 1. 2 とする。また、通信相手装置 B 11-2 の IP アドレスとしては、133. 134. 10. 10 として説明を行う。なお、以上の IP アドレスの値はあくまでも一例であり、他のアドレスであっても問題ない。

【0030】

以下、図 3 ～図 9 を用いて通信相手装置 A 11-1 との通信方法を説明し、図

10～図13を用いて通信相手装置B11-2との通信方法を説明する。

【0031】

まず、社内ネットワーク2のみを介した通信装置10と通信相手装置A11-1との通信方法を説明する。図3は、利用者9が通信装置10を用いて通信相手装置A11-1とピアツーピア通信を開始する際のメッセージシーケンスである。

【0032】

利用者9は、まず通信装置10に対し、図1に示す周辺機器20からセキュリティポリプレゼンス情報要求指示I/F403を介して、通信相手装置A11-1のセキュリティポリシおよびプレゼンス情報の取得を指示する501。指示を受けた通信装置10は、通信相手装置A11-1にプレゼンス情報およびセキュリティポリシを要求するメッセージをピアツーピア通信機能ブロック200にて生成し、IP機能ブロック100を介してIPパケットに載せて送信する502。

【0033】

本パケットは通常のデータパケットと異なり、セキュリティポリシを交換するためのパケットであり、例えばInternet-Draft (draft-IETF-imp-p-c-pim-pidf-07.txt)で規定されたフォーマットで生成されている。したがって、このIPパケットが受信側の通信相手装置A11-1のセキュリティポリシを満たしているかは不明であるが、この段階では受信側装置で廃棄されることなく受信される。

【0034】

本要求メッセージを受信した通信相手装置A11-1は、プレゼンス情報およびセキュリティポリシを応答メッセージとしてIPパケットに載せて返信する503。通信装置10は上記通信相手装置A11-1からの応答メッセージが載せられたIPパケットを受信すると、プレゼンス情報処理部401にて受信パケットの内容を解析することによって、相手通信装置A11-1のプレゼンス情報を抽出し、プレゼンス情報データベース400に登録する504。そしてプレゼンス情報入出力I/F402から周辺機器20を用いて、通信相手装置A11aの

プレゼンス情報を利用者 9 に対して表示する 505。

【0035】

同様に、通信相手装置 A11-1 からの応答パケットをセキュリティポリシ処理部 301 にて解析することによって通信相手装置 A11-1 のセキュリティポリシデータを抽出し、セキュリティポリシ入出力 I/F 302 から周辺機器 20 を用い当該セキュリティポリシを利用者 9 に対して表示する 506。

【0036】

利用者 9 は、表示された通信相手装置 A11-1 における通信装置 10 に対するセキュリティポリシの内容を検討し必要に応じて変更する。例えば、セキュリティレベルをより高く変更したり、あるいは低くする等を行う。

【0037】

前記のように内容が見直されたセキュリティポリシは、セキュリティポリシ入出力 I/F 302 から周辺機器 20 を用い登録される 507。登録の指示を受けた通信装置 10 は、上記の通信相手装置 A に対するセキュリティポリシを、セキュリティポリシ処理部 301 を介してセキュリティポリシデータベース 300 に登録する 508。

【0038】

その後、利用者 9 はピアツーピア通信機能ブロック 200 を介して通信相手装置 A11-1 とのピアツーピア通信の開始を指示し 509、指示を受けた通信装置 10 は、前記ピアツーピア通信機能ブロック 200 を用いて通信相手装置 A11-1 とのピアツーピア通信を開始する 510。

【0039】

ピアツーピア通信機能ブロック 200 には、周辺機器あるいは図示しない外部の装置や端末等から、通信相手装置に向けた通常の通信データが入力され、IPsec 機能ブロックとの間で、相手装置との送受信データの IP アドレスやポート番号、上位プロトコルの種別を受渡しすることによって、セキュリティポリシデータベース 300 に登録された前記セキュリティポリシに基づいたデータパケットが生成される。

【0040】

図4は、図3のシーケンスにおける通信相手装置A11-1のセキュリティポリシおよびプレゼンス情報要求指示時501にて、セキュリティポリシプレゼンス情報要求指示I/F403が周辺機器20のディスプレイ装置等に提供するGUI（グラフィカルユーザインタフェース）410の一例である。通信相手装置のアドレスをテキストボックス411に入力し、要求する情報のチェックボックス412、413をチェックし、OKボタン414を押すことで要求を指示する。

【0041】

図5に、図3のシーケンスにおける、通信相手装置A11-1からのプレゼンス情報およびセキュリティポリシ情報の応答503におけるプレゼンス情報およびセキュリティポリシの記述部分の一例を示す。ここでは、IETF（Internet Engineering Task Force）のIMPP（Instant Messaging and Presence Protocol）WG（Working Group）にて作成中であるPIDF（Presence Information Data Format）に準拠したフォーマットで作成されている。

【0042】

図5において、520～526がセキュリティポリシに関する情報であり、527～528がプレゼンス情報である。なお、本メッセージは、例えばIETFのRFC（Request for Comments）3261に規定されたSIPに代表されるピアツーピア通信プロトコルを用いて送受信が可能である。

【0043】

図6は、図3のシーケンスにおいて通信相手装置A11-1のプレゼンス情報をプレゼンス情報データベース400に登録した時504における、プレゼンス情報データベース400の内容の一例である。各要素は、関連する通信装置のプレゼンス情報に対応し、端末の識別情報であるentity620、端末のアドレス621、端末の現在の利用者名622、端末のある場所623、本プレゼンス情報が作成された日時624の各行から構成される。ここでは、625および627～629がそれぞれ図5のメッセージの530および527～529に対

応する。

【 0 0 4 4 】

図 7 は、図 3 のシーケンスにおいて通信相手装置 A 1 1 - 1 に対するセキュリティポリシをセキュリティポリシデータベース 3 0 0 に登録した時 5 0 8 のセキュリティポリシデータベース 3 0 0 内容の一例である。各要素は通信相手装置 1 1 に対するセキュリティポリシに対応し、送信元のアドレス 7 1 0 とそのポート番号 7 1 1、送信先のアドレス 7 1 2 とそのポート番号 7 1 3、トランスポート層のプロトコル 7 1 4、送信か受信かを示す方向 7 1 5、パケットに対してどのような処理を行うかを示すアクション 7 1 6 がある。

【 0 0 4 5 】

また、アクションにて i p s e c を指定した場合についてはさらに、プロトコル 7 1 7、モード 7 1 8、エンドポイント 7 1 9、レベル 7 2 0 の各行から構成される。ここでは、7 2 1 ~ 7 2 7 がそれぞれ図 5 のメッセージの 5 1 0 ~ 5 1 6 に対応する。

【 0 0 4 6 】

図 8 に、前記通信相手装置 A 1 1 - 1 との間のセキュリティポリシを表示した時 5 0 6 における、セキュリティポリシ入出力 I / F 3 0 2 が周辺機器 2 0 のディスプレイ装置等に提供する G U I 8 0 0 の一例を示す。送信元および送信先のアドレスは、それぞれテキストボックス 8 1 0 および 8 1 4 に表示される。

【 0 0 4 7 】

特定のポートが指定されている場合は、テキストボックスのチェックボックス 8 1 1 および 8 1 5 が選択され、テキストボックス 8 1 2 および 8 1 6 に具体的なポート番号が表示される。特定のポートが指定されていない場合には a n y のチェックボックス 8 1 3 および 8 1 7 が選択される。

【 0 0 4 8 】

トランスポート層のプロトコルは、対応するプロトコル名のラジオボタン 8 1 8 または 8 1 9 が選択される。プロトコルが指定されていない場合は a n y のラジオボタン 8 2 0 が選択される。パケットの送信方向は、受信パケットならば i n のラジオボタン 8 2 1 が選択され、送信方向ならば o u t のラジオボタン 8 2

2 が選択される。

【0049】

パケットに対する処理については、パケット廃棄処理を行うならば `discard` のラジオボタン 823 が選択され、何も処理を行わないのであれば `none` のラジオボタン 824 が選択され、`ipsec` 処理を行うならば `ipsec` のラジオボタン 825 が選択される。

【0050】

`ipsec` のラジオボタンが選択されている場合には、さらに、適用するセキュリティプロトコルである `ah` (認証) 826、`esp` (暗号) 827、`ipcomp` (圧縮) 828 のそれぞれのチェックボックスが選択される。適用するモードがトランスポートモードかトンネルモードかはラジオボタン 829 または 830 を選択する。トンネルモードの場合は、トンネルのもう一方の端となる装置を示すテキストボックス 831 が表示され、セキュリティレベルとして `default` (デフォルト) 832、`use` (可能ならば) 833、`require` (必須) 834 のそれぞれのラジオボタンが表示される。

【0051】

図 8 では、通信相手装置 A11-1 から受け取ったセキュリティポリシを元に、通信相手装置 A11-1 に対するセキュリティポリシとして、送信元アドレス 192.168.1.1、ポート `any`、送信先アドレス 192.168.1.2、ポート `any`、トランスポート `udp`、方向 `out`、アクション `none` がそれぞれ選択され、表示されている。通信相手装置 A11-1 は社内 IP ネットワークに接続されているので、利用者はセキュリティポリシの変更は不要と判断し、このままのセキュリティポリシで登録ボタン 835 を押し、セキュリティポリシデータベースに登録を行う。

【0052】

図 9 に前記通信相手装置 A11-1 のプレゼンス情報を表示した時 505 における、プレゼンス情報入出力 I/F 402 が周辺機器のディスプレイ装置等に提供する GUI 900 の一例を示す。

【0053】

端末の識別情報である `entity 910`、端末のアドレス `911`、端末の現在の利用者 `912`、端末のある場所 `913`、プレゼンス情報が作成された日時 `914` がそれぞれ表示される。図 9 では、通信相手装置 A から受け取ったプレゼンス情報として、`entity peer A@example.com 917`、アドレス `192.168.1.2 (918)`、利用者 `John 919`、場所 `office 920`、日時 `2002-09-28 10:49:29 (921)` がそれぞれ表示されている。したがって、通信装置の利用者は、通信装置 A 11-1 が社内 IP ネットワークに接続されていることを知ることができる。

【0054】

なお、通信相手装置 A 11-1 のプレゼンス情報はプレゼンス情報要求時にプレゼンス情報データベースに登録される。利用者はプレゼンス情報入出力 I/F を用いて、通信相手装置 A 11-1 のプレゼンス情報のうち、利用者と場所の欄のみ利用者の好みに応じて親しみやすい値等に変更することが出来る。

【0055】

次に、社内 IP ネットワーク 2 とインターネット 3 とを介した通信装置 10 と通信相手装置 B 11-2 との通信方法を説明する。図 10 は、利用者 9 が通信装置 10 を用いて通信相手装置 B 11-2 とピアツーピア通信を開始する際のメッセージシーケンスである。利用者 9 は、前述の通信装置 A 11-1 と通信を行う場合と同様、通信装置 10 に対し前記セキュリティポリシープレゼンス情報要求指示 I/F 403 が周辺機器 20 のディスプレイ装置等に提供する GUI 等を用いて、通信相手装置 B 11-2 のセキュリティポリシーおよびプレゼンス情報の要求を指示する 601。

【0056】

指示を受けた通信装置 10 は、通信相手装置 B 11-2 にプレゼンス情報およびセキュリティポリシーを要求するメッセージを送信する 602。通信相手装置 B 11-2 はプレゼンス情報およびセキュリティポリシーを応答するメッセージを返信する 603。

【0057】

応答メッセージを受信した通信装置 10 は、通信相手装置 B 11-2 のプレゼ

ンス情報を前記プレゼンス情報データベース 4 0 0 に登録し 6 0 4、前記プレゼンス情報入出力 I / F 4 0 2 を用いて周辺機器 2 0 のディスプレイ装置等に通信相手装置 B 1 1 - 2 のプレゼンス情報を表示する 6 0 5。また、前記セキュリティポリシ入出力 I / F 3 0 2 を用いて周辺機器 2 0 のディスプレイ装置等に通信相手装置 B 1 1 - 2 との間のセキュリティポリシを表示する 6 0 6。以上は前述の図 3 に示した社内 I P ネットワーク 2 を介した通信相手装置 A 1 1 - 1 とのメッセージシーケンスと同一である。

【 0 0 5 8 】

ここで、利用者 9 は表示された通信相手装置 B 1 1 - 2 のプレゼンス情報を解析することによって、通信相手装置 B 1 1 - 2 の現状の接続先が社外のネットワークであることが分かる。

【 0 0 5 9 】

図 1 1 は、図 1 0 のシーケンスにおいて前記通信相手装置 B のプレゼンス情報を表示した時 6 0 5 の、外部のディスプレイ装置への G U I 1 1 0 の一例である。場所 9 3 0 が s t a t i o n となっており、通信相手装置 B 1 1 - 2 が社外ネットワークに接続されていることが判る。そこで、別途表示された通信相手装置 B 1 1 - 2 との間のセキュリティポリシの内容を解析し、セキュリティレベルが現状に相応なものか否かを判断する。

【 0 0 6 0 】

図 1 2 は、このときのセキュリティポリシの外部ディスプレイ装置への G U I 1 2 0 0 の一例である。通信パケットに対する処理が n o n e 8 5 0 となっているため、通信パケットに対するセキュリティ処理を行わないポリシであることを示している。なお、これは図 8 に示した社内 I P ネットワークのみを介した通信を前提としたセキュリティポリシと同等である。

【 0 0 6 1 】

このような場合、通信の安全性を確保するためのセキュリティポリシとしては十分でないと判断し、図 1 0 のシーケンス 6 0 8 に示すように、利用者 9 は通信相手装置 B 1 1 - 2 に対するセキュリティポリシをレベルのより高いものに変更する。そして利用者 9 は通信装置 1 0 に対して、その変更後のセキュリティポリ

シの登録を指示し 6 0 9、指示を受けた通信装置 1 0 は、前記セキュリティポリシーデータベース 3 0 0 に登録する 6 1 0。

【 0 0 6 2 】

図 1 3 はこの変更時における、セキュリティポリシーの外部ディスプレイ装置への G U I 1 3 0 0 の一例である。すなわち、先の図 1 1 が変更前、本図 1 3 が変更後に相当するものである。通信相手装置 B 1 1 - 2 のプレゼンス情報から通信相手装置 B 1 1 - 2 が社外ネットワークに接続していることが明らかとなったため、通信相手装置 B 1 1 - 2 への送信パケットに対して、セキュリティ処理 (i p s e c 8 6 0) を行うこととし、認証 (a h 8 6 1)、暗号化 (e s p 8 6 2) を必須 (r e q u i r e 8 6 5) としていることを示している。

【 0 0 6 3 】

その後、利用者 9 は通信相手装置 B 1 1 - 2 とのピアツーピア通信の開始を指示し 6 1 1、指示を受けた通信装置 1 0 は、前記ピアツーピア通信機能ブロック 2 0 0 を用いて通信相手装置 B 1 1 - 2 とのピアツーピア通信を開始する 6 1 2。

【 0 0 6 4 】

ここで、通信相手装置 B 1 1 - 2 が保持している通信装置 1 0 からの受信パケットに関するセキュリティポリシー (S P 1) と、通信装置 1 0 が保持している通信相手装置 B 1 1 - 2 への送信パケットに関するセキュリティポリシー (S P 2) とを比較すると、S P 1 に比べて S P 2 の方がそのセキュリティレベルが高いものとなっている。

【 0 0 6 5 】

しかしながら、受信側 (通信相手装置 B 1 1 - 2) で設定している以上のセキュリティレベルで送信されたパケットについては、受信側でそのまま受信してもセキュリティ上の問題はない。したがって、通信に先立って通信装置 1 0 から通信相手装置 B 1 1 - 2 に対してセキュリティポリシーの変更やそのネゴシエーションを実施することは必ずしも必要でない。

【 0 0 6 6 】

これに対して、前述のセキュリティポリシーの変更時 6 0 8 において、変更後の

セキュリティポリシーのセキュリティレベルが通信相手装置 B 1 1 - 2 にて保持するものと比して低くなるよう変更した場合、通信相手装置 B 1 1 - 2 では自ら設定しているより低いセキュリティレベルの受信パケットは廃棄等の処理が行われるため、通信装置 1 0 は通信に先立って通信相手装置 B 1 1 - 2 とセキュリティポリシーの変更に関してネゴシエーションが必要となる。

【 0 0 6 7 】

なお、以上の実施例では、セキュリティ通信プロトコルとして I P s e c を前提として説明を行ったが、I P s e c 機能ブロックを置き換えることによって、他のセキュリティ通信プロトコルにも適用可能である。また、セキュリティポリシーデータベースやプレゼンス情報データベースは必ずしもデータベースである必要はなく、メモリ上のテーブルでも実現可能である。

【 0 0 6 8 】

【発明の効果】

以上のように本発明によれば、ピアツーピア通信において通信端末や使用者の状況に応じた適切なセキュリティポリシーを用いた通信が可能となる。また、適切なセキュリティポリシーを選択可能とすることにより、過剰なセキュリティレベルでのピアツーピア通信を防ぎ、通信端末での C P U リソースや通信ネットワークの帯域の節約が可能となる。

【図面の簡単な説明】

【図 1】

本発明の通信装置の内部ブロック図を説明する図である。

【図 2】

本発明の通信装置の適用されるネットワーク構成を説明する図である。

【図 3】

本発明のメッセージシーケンスを説明する図である。

【図 4】

本発明の G U I 表示の一例を説明する図である。

【図 5】

本発明のプレゼンス情報およびセキュリティポリシーの記述部分を説明する図で

ある。

【図 6】

本発明のプレゼンス情報データベースの構成を説明する図である。

【図 7】

本発明のセキュリティポリシデータベースの構成を説明する図である。

【図 8】

本発明の G U I 表示の一例を説明する図である。

【図 9】

本発明の G U I 表示の一例を説明する図である。

【図 10】

本発明のメッセージシーケンスを説明する図である。

【図 11】

本発明の G U I 表示の一例を説明する図である。

【図 12】

本発明の G U I 表示の一例を説明する図である。

【図 13】

本発明の G U I 表示の一例を説明する図である。

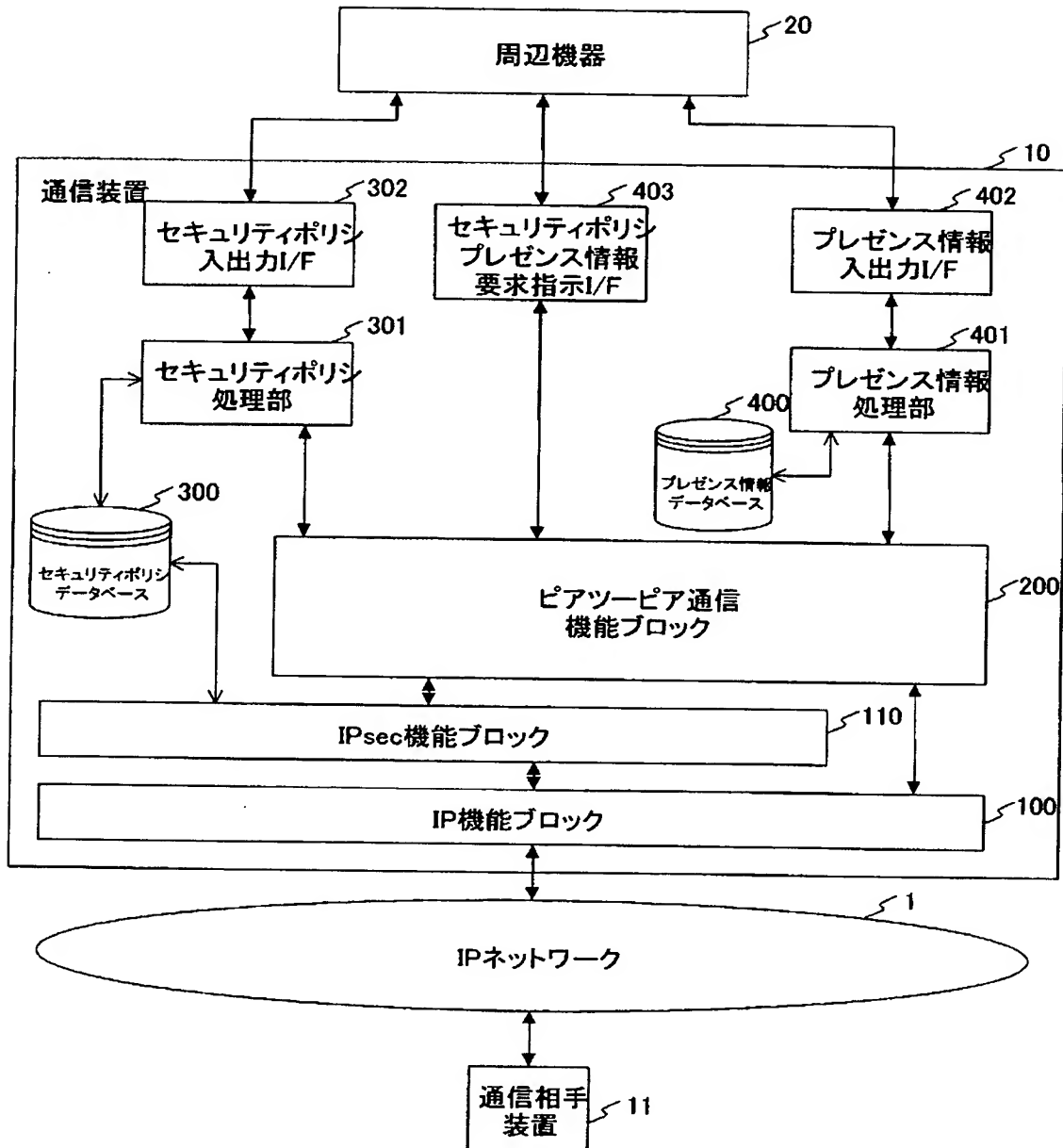
【符号の説明】

1・・・IPネットワーク、2・・・社内ネットワーク、3・・・インターネット、9・・・利用者、10・・・通信装置、11・・・通信相手装置、100・・・IP機能ブロック、110・・・IPsec機能ブロック、200・・・ピアツーピア通信機能ブロック、300・・・セキュリティポリシデータベース、301・・・セキュリティポリシ処理部、302・・・セキュリティポリシ入出力I/F、400・・・プレゼンス情報データベース、401・・・プレゼンス情報処理部、402・・・プレゼンス情報入出力I/F、403・・・セキュリティポリシプレゼンス情報要求指示I/F

【書類名】 図面

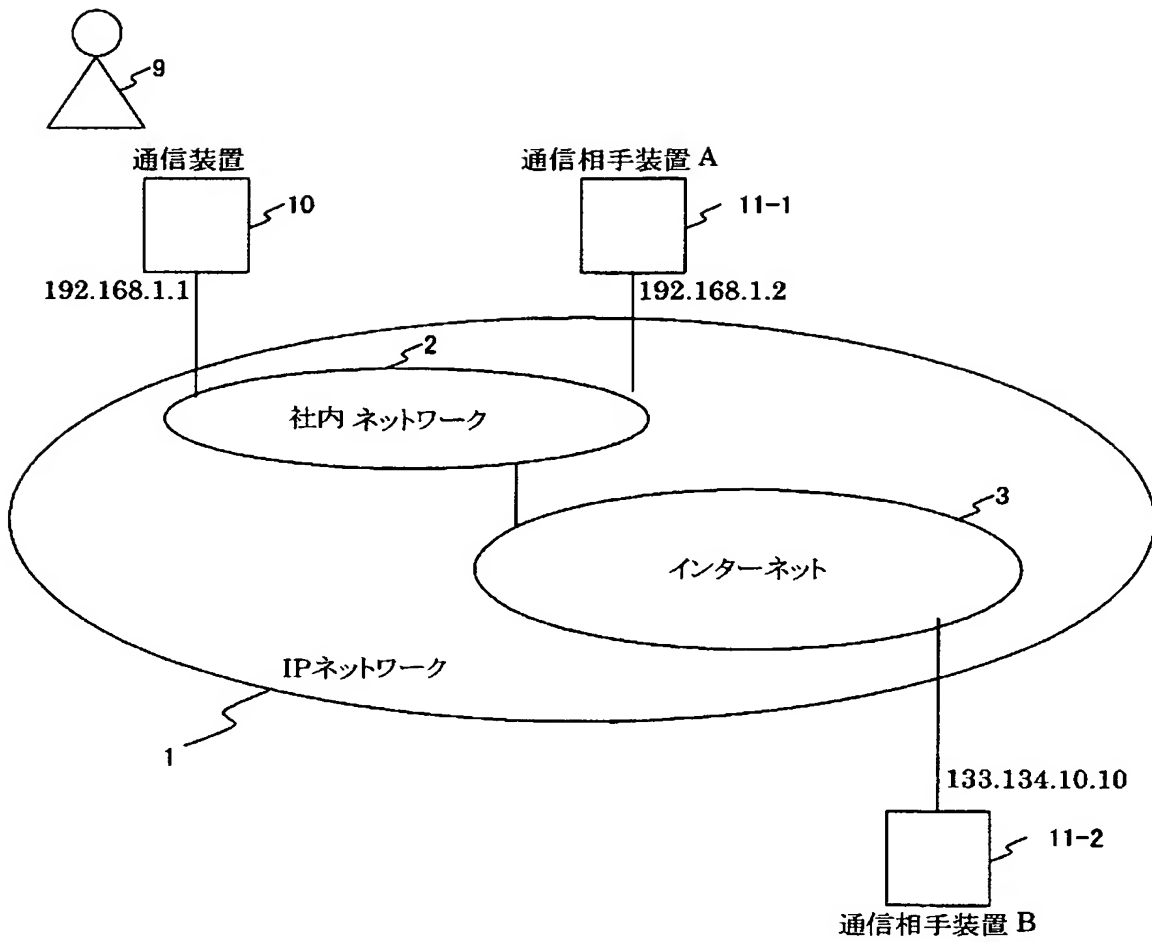
【図 1】

【図 1】



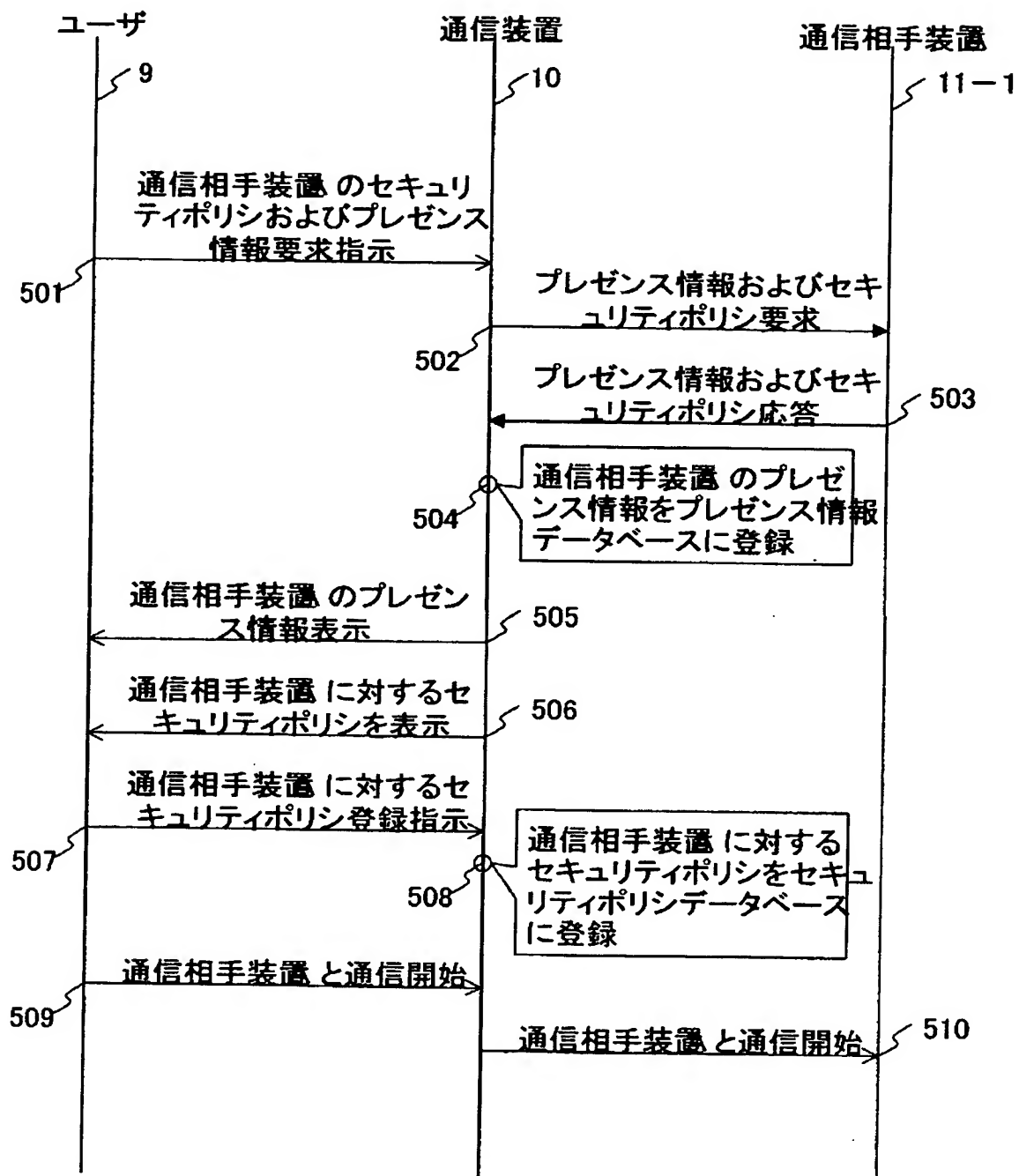
【図 2】

【図2】



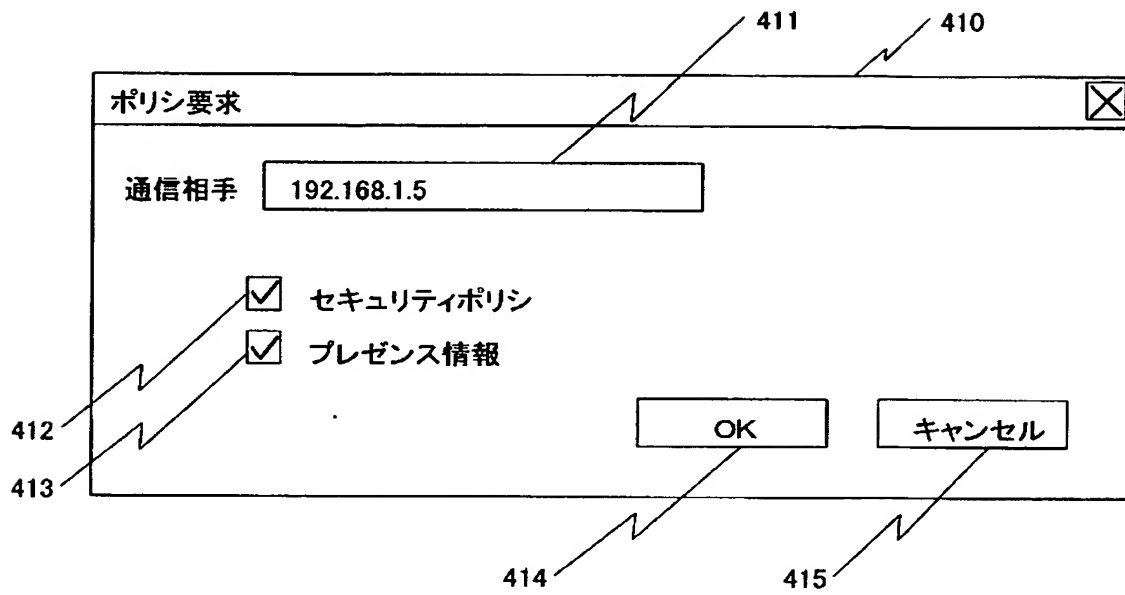
【図 3】

【図3】



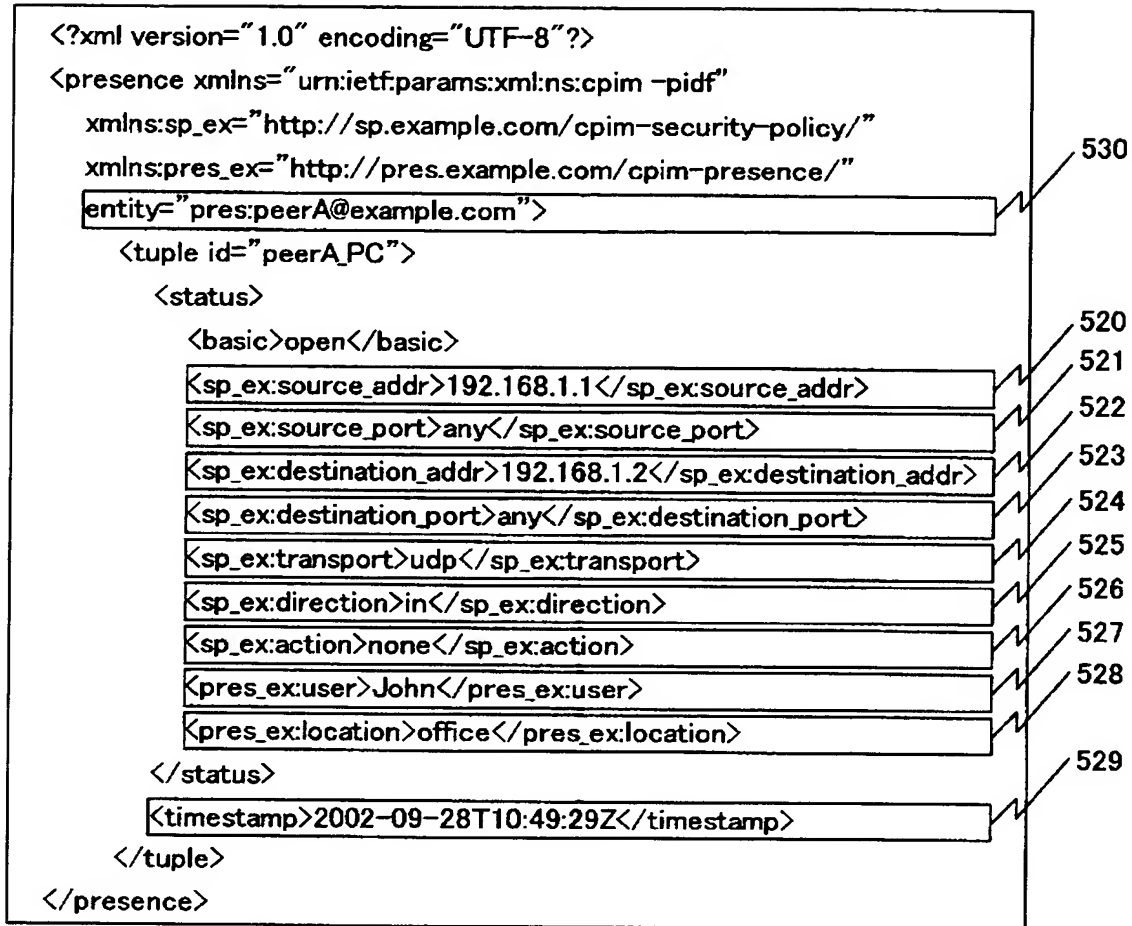
【図 4】

【図4】



【図 5】

【図5】



【図 6】

【図6】

entity	アドレス	利用者	場所	日時
peerA@example.com	196.128.1.2	John	office	2002-09-28 10:49:29
...

【図 7】

【図7】

送信元		送信元		トランスポート	方向	アクション	プロトコル	モード	エンドポイント	レベル
アドレス	ポート	アドレス	ポート	ポート						
192.168.1.1	any	192.168.1.2	any	udp	out	none	—	—	—	—
...

【図 8】

【図 8】

800

ポリシー情報

セキュリティポリシー

送信元アドレス 192.168.1.1

送信先アドレス 192.168.1.2

ポート: any

ポート: any

818

821

トランスポート: tcp, udp, any

方向: in, out

アクション: discard, none, ipsec

823

824

825

プロトコル: ah, esp, ipcomp

モード: transport, tunnel

エンドポイント

レベル: default, use, require

832

833

834

登録

キャンセル

835

836

810

811

812

813

814

815

816

817

819

820

822

826

827

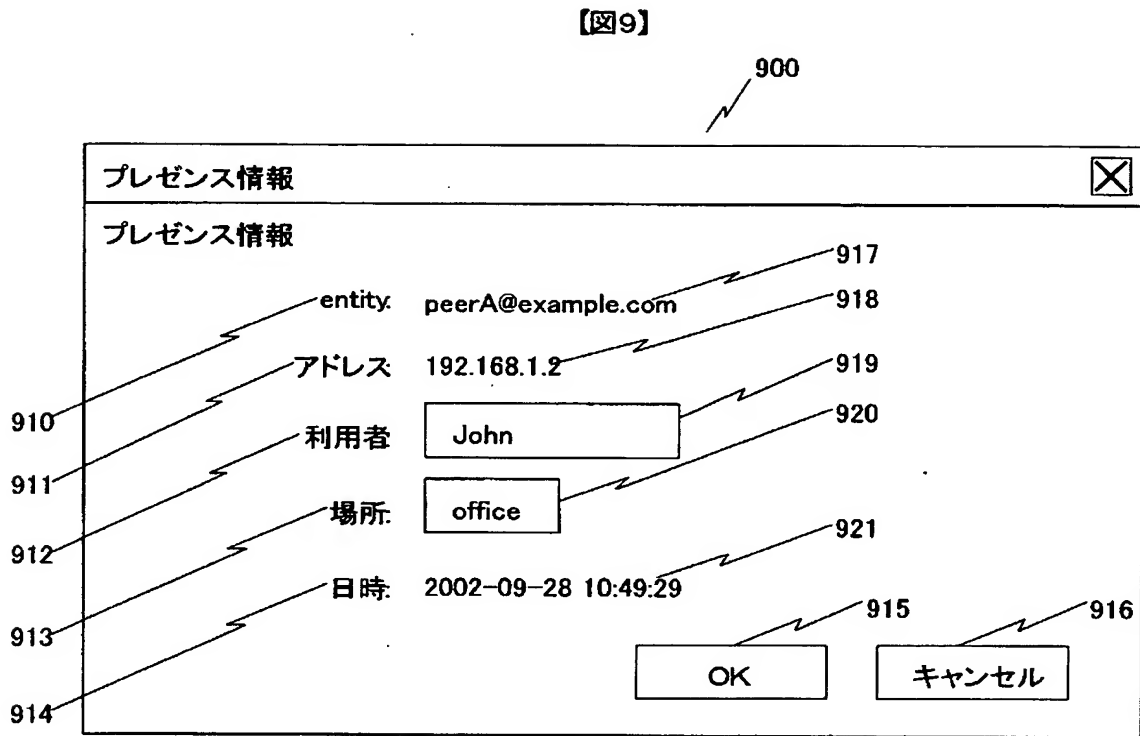
828

829

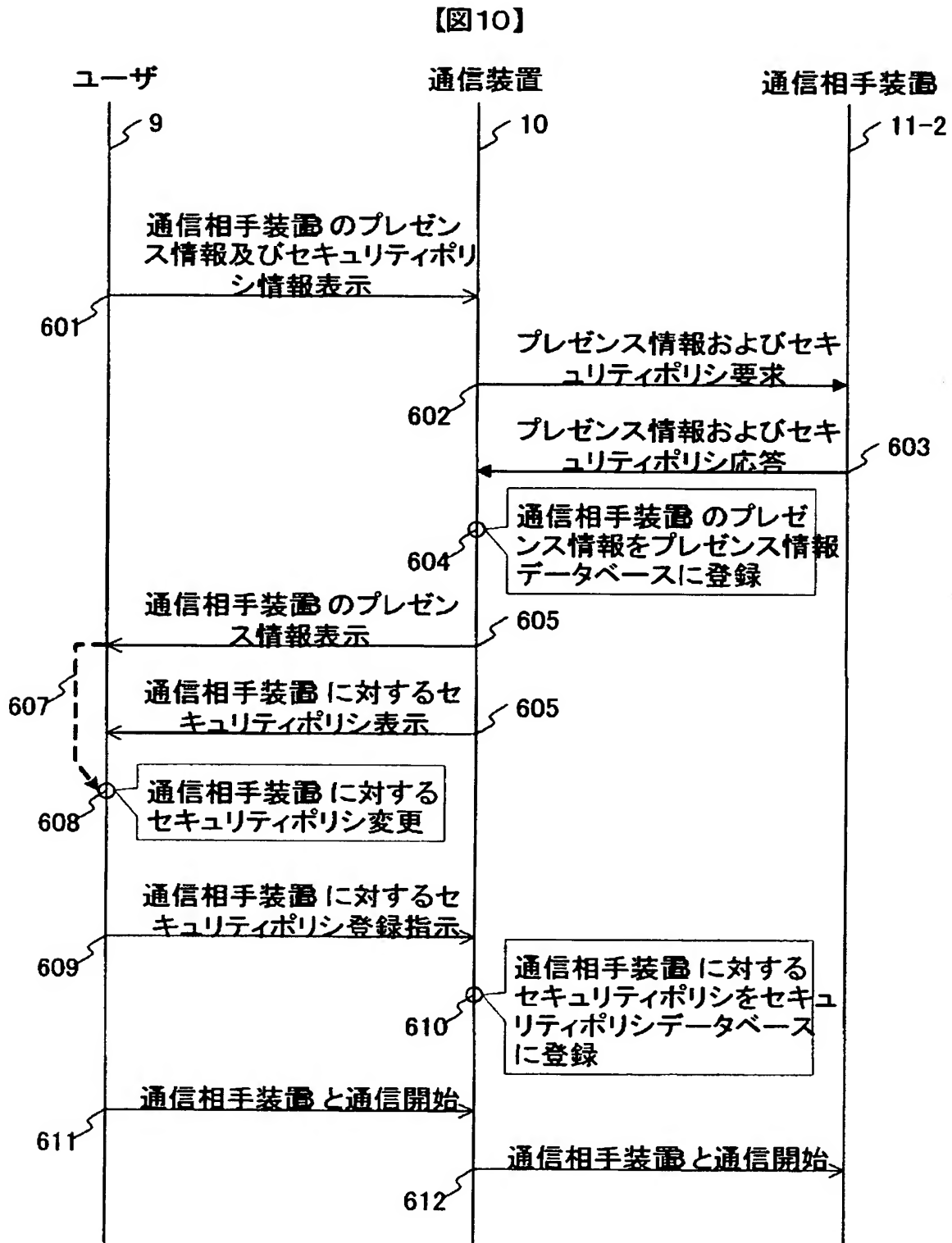
830

831

【図 9】



【図10】



【図 11】

【図11】

1100

プレゼンス情報

プレゼンス情報

entity: peerB@example.com

アドレス 133.134.10.10

利用者

場所

930

日時: 2002-09-28 16:15:46

OK キャンセル

【図 1 2】

【図12】

1200

ポリシー情報 ✕

セキュリティポリシー

送信元アドレス ポート: ☐ ☒ any

送信先アドレス ポート: ☐ ☒ any

トランスポート ☐ tcp ☒ udp ☐ any

方向: ☐ in ☒ out

アクション ☐ discard

850 ↗ ☒ none

☐ ipsec

プロトコル ☐ ah ☐ esp ☐ ipcomp

モード ☐ transport ☐ tunnel

エンドポイント

レベル ☐ default ☐ use ☐ require

【図13】

【図13】

1300

ポリシー情報

セキュリティポリシー

送信元アドレス 192.168.1.1 ポート: ☐ ☒ any

送信先アドレス 133.134.10.10 ポート: ☐ ☒ any

トランスポート ☐ tcp ☒ udp ☐ any

方向 ☐ in ☒ out

アクション ☐ discard
☐ none
☒ ipsec

860

プロトコル ☒ ah ☒ esp ☐ ipcomp

861 864 862 863

モード ☐ transport ☐ tunnel

エンドポイント

レベル ☐ default ☐ use ☒ require

865

登録 キャンセル

866

【書類名】 要約書

【要約】

【課題】

安全性が確保されたピアツーピア通信を実現するために、通信パケットに対する暗号および認証規則を示すセキュリティポリシおよび通信装置の通信状況を示すプレゼンス情報を通信装置間で互いに交換し、通信状況に応じた適切なセキュリティポリシを用いたセキュアなピアツーピア通信を可能とする通信装置を提供する。

【解決手段】

I P ネットワークに接続された他の通信装置が属するネットワークおよび前記他の通信装置の利用者に関するプレゼンス情報を取得する手段と、前記他の通信装置の通信パケットの送受信における一連の暗号および認証規則を示すセキュリティポリシ情報を取得する手段とを備え、前記プレゼンス情報と前記セキュリティポリシ情報とから、前記他の通信装置に送信する I P パケットのセキュリティポリシを決定し、前記決定したセキュリティポリシを用いて前記他の通信装置に I P パケットを送信する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 6 4 3 2 8
受付番号	5 0 3 0 0 3 8 9 5 3 7
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 5 年 3 月 1 2 日

< 認定情報・付加情報 >

【提出日】	平成15年 3月11日
-------	-------------

次頁無

特願 2 0 0 3 - 0 6 4 3 2 8

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1 . 変 更 年 月 日 1 9 9 0 年 8 月 3 1 日

[変 更 理 由] 新 規 登 録

住 所 東 京 都 千 代 田 区 神 田 駿 河 台 4 丁 目 6 番 地
氏 名 株 式 会 社 日 立 製 作 所